REMARKS/ARGUMENTS

Section 102(b)

The office action has rejected independent claim 98 under 35 U.S.C. 102(b) as being anticipated by Bapat (U.S. Pat. No. 6,038,563). Claim 98 has been amended to help clarify the exact bounds of the invention.

For a prior art reference to anticipate in terms of 35 U.S.C. § 102, anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim. *Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick Co.*, 730 F.2d 1452, 1458 (Fed. Cir. 1984). Applicant respectfully points out that Bapat does not disclose each and every element of the claimed invention, arranged as in the claim.

The office action cites the log server 290 of Bapat as disclosing the limitation registering a listener agent with the console. The following limitation, registering a listener agent with the console, is cited to a set of filters 291, 294 in the log server 290. For the next limitation, establishing a secure connection between the console and the listener agent, Bapat Figure 3 is cited. However, applicant cannot discern in Figure 3 any structure corresponding to the cited disclosures concerning the log server and filters. Applicant believes that the disclosed structure of Bapat does not anticipate the limitations concerning the listener agent and its relationship with the console.

The next limitation, configuring the listener agent with a first set of rules having a set of security attributes, is cited to Bapat's filter 291 passing "access grant" and "access denial" event notifications generated by the MIS. Applicant does not believe that the

limitation reads on the cited portion of Bapat, or that the listener agent of the present invention is a log server with filters.

The next limitation, installing a collector agent to be in communication with the listener agent for collecting a plurality of database events, the office action again cites the language of Bapat that the filter 291 passes "access grant" and "access denial" event notifications generated by the MIS. Applicant does not believe that collecting events through a collector and listener is met by Bapat's passing access grant and access denial event notifications.

The next limitation, deconstructing the plurality of database events into a plurality of atomic messages, is cited to user queries requesting information from tables to which the user does not have access rights are rejected by the SQL engine. Applicant does not see how this claim step of deconstructing is met by rejection by the SQL engine for users without access rights.

The next limitation, analyzing the plurality of database events into a plurality of atomic messages, the office action cites Bapat for a security alarm log 293 that is separate from the security audit trail 192, where security alarms are generated and stored in the log only when there is a denial of object access. Applicant respectfully suggests that the step of analyzing database events into atomic messages is not met by a security alarm log.

The next limitation, executing compliant database events, depends on the term "compliant" in the context of analysis of atomic messages. The cited section of Bapat merely states the object of every security system, i.e., that access rights are granted only when the user has appropriate access rights.

The next limitation, sending a signal to a console operator when a database event is not compliant with the first set of rules, is cited to Bapat's disclosure that if a match is found, the request is denied, and a response is returned to the initiator if appropriate. Again, applicant does not see a signal being sent to a console operator when an event is not compliant with a first set of rules.

The next limitation, allowing a console operator to create exceptions when signals are sent by the listening agent, is cited to users authorized to modify the access control tree. The general proposition that someone is authorized to modify the access control tree of Bapat is not the step of allowing a console operator to create exceptions. This limitation has been amended to reflect the change is to the first set of rules.

The next limitation, updating the first set of rules with the exceptions created by the console operator, is cited to users authorized to modify the access control tree. The limitation is a step; updating the rules created by the console operator. The Bapat disclosure merely states that there are users authorized to modify the access control tree. This does not meet the limitation of the instant process step.

The next and last limitation, storing the signals received by the console operator in a data file residing with the console, is cited to the deny/grant decision for each access request may be stored in a security audit trail. The cited portion of Bapat does not disclose storing the signals received by the console operator, nor that the data file resides with the console, and thus this limitation is not anticipated by the cited disclosure.
In view of these considerations, it is respectfully submitted that the rejection of claim 98 should be withdrawn.

Section 103

It is noted that the Examiner has rejected claims 99 - 104as being unpatentable over Bapat in view of a number of different references. Those references include Shostack, (U.S. Patent No. 6,298,445) hereinafter referred to as Shostack; Reshef (U.S. Pat. No. 6,321,337) hereinafter referred to as Reshef; and Rowland (U.S. Pat. No. 6,405,318) hereinafter referred to as Rowland.

Dependent claim 99: Shostack does not teach the implementation of a buffer overflow analysis at the database level. The present invention is directed to database level, SQL analysis, which is not taught or suggested by Shotack.

Dependent claim 100: Reshef is cited for detecting whether an executable SQL statement includes an operating system call, where Reshef merely states that "[a]ny breach of the permitted flow sequences by disorderly operating system calls or looping will be trapped and logged." Reshef does not teach or disclose the analysis of the present invention, which applies to SQL statements for a system that resides at the database level.

Dependent claim 101: Applicants note that claim 101 depends from claim 98, and therefore is not an independent claim. The citation to Bapat does not show specifically the subject matter of claim 101, i.e., that the particular SQL statement is a write operation to a data dictionary, rather, the citation merely states that a suspicious directory name would generate a notification, with a subsequent rejection if a match is found.

Dependent claims 102-104: Rowland is not a compatible structure or method with the present invention. Rowland is directed to intercepting activity at the IP/TCP level, and not at the database level. Rowland does not disclose any method of analyzing SQL statements at the database level, which is the purpose of the present invention.

Non-Analogous Art

Applicant respectfully requests that the examiner reconsider the decision that Reshef is analogous art. Applicant maintains that the reference is nonanalagous art because Reshef concerns a security gateway system positioned between an external, untrusted computing environment and an internal, trusted computing environment, and does not concern security at the database level through analysis of SQL statements.

CONCLUSION

Applicants believe that the above places the application in a condition for allowance.

Respectfully submitted,

Law Offices of Peter S. Canelias September 16, 2008

By: 

Peter S. Canelias
Reg. No. 40,547
Law Offices of Peter S. Canelias
420 Lexington Avenue-Suite 2620
New York, NY 10170
Tel: (212) 223-9654
Fax: (212) 223-9651